

**WEB应用防火墙详细使用手册**

****

**HTTPWAF研发团队**

**https://gitee.com/httpwaf/**

**版权声明**

本文所有解释权归HTTPWAF研发部所有

HTTPWAF（下文简称WAF）版权所有，保留一切权利。

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**开发团队**所有，受到有关产权及版权法保护。未经书面许可不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。

**信息更新**

本文档仅用于为最终用户提供帮助信息，并且随时可由更改或撤回，以最新的文档为准。

**适用版本**

**本文档适用于最新发布版本。**

**免责条款**

根据适用法律的许可范围，按“最新发布版本”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

**期望读者**

期望了解本产品主要技术特性的用户、研发人员、售前人员、代理商成员等。本文档假设您对下面的知识有一定的了解：

* HTTP与HTTPS协议
* Linux基础知识
* 网络安全基础知识
* 文档信息

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** |  | | |
| **扩散范围** | 可扩散任何人 | **文档版本号** | 2.0 |
| **作者** |  | **日期** |  |
| **初审人** |  | **复审人** |  |

* 版本变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| **时间** | **版本** | **说明** | **作者** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1. 安装前准备 6](#_Toc28125)

[1.1. 系统支持 6](#_Toc21507)

[1.2. 承诺 6](#_Toc15437)

[1.3. 不承诺 6](#_Toc21738)

[2. 部署方式 7](#_Toc29078)

[2.1. 模式一：直接安装在WEB服务器上 7](#_Toc5948)

[2.2. 模式二：独立部署，反向代理后端WEB服务器 7](#_Toc26043)

[2.3. 安装步骤 7](#_Toc25751)

[2.4. 运行、停止和卸载 8](#_Toc28393)

[3. WEB管理 9](#_Toc10610)

[3.1. 登录 9](#_Toc25290)

[3.2. 主页 9](#_Toc23446)

[4. 基本设置 11](#_Toc9127)

[4.1. 服务器设置 11](#_Toc4419)

[4.2. 规则管理 12](#_Toc8049)

[4.3. 自定义规则 12](#_Toc13971)

[4.4. 系统设置 15](#_Toc6175)

[4.5. IP封禁设置 16](#_Toc31446)

[5. 黑白名单 16](#_Toc2062)

[5.1. URL白名单 17](#_Toc7682)

[5.2. IP白名单 17](#_Toc19008)

[6. 日志查看 18](#_Toc18027)

[6.1. 攻击日志 18](#_Toc11690)

[6.2. 溯源日志 19](#_Toc2391)

[6.3. 封禁日志 20](#_Toc5117)

[6.4. 未知漏洞【收费】 20](#_Toc25910)

[7. 统计分析 21](#_Toc32639)

[7.1. IP流量统计 21](#_Toc8826)

[7.2. URL分析统计 21](#_Toc20726)

[7.3. 十大攻击源 21](#_Toc30829)

[8. 系统管理 22](#_Toc15799)

[8.1. 远程管理 22](#_Toc32117)

[8.2. 恢复出厂设置 23](#_Toc1876)

[8.3. 系统重启 23](#_Toc26272)

[9. 开机启动 23](#_Toc2423)

[10. 开放源码 23](#_Toc30832)

# 安装前准备

## 系统支持

HTTPWAF是一款对抗未知攻击为的WEB应用防火墙，支持CentOS、Ubuntu、Debian、OpenEuler、Fedora等Linux x86-64位原生系统，确认下面三个端口没被占用：

80对外提供HTTP服务，可修改。

443对外提供HTTPS服务，可修改。

9999管理端口，不可修改，禁止向公网开放（或设置IP访问白名单）。

## 承诺

1. 和云WAF不一样，为了保证服务器安全，我们承诺：除首次下载安装包，**任何时候绝不联网**，更没有任何后门，不放心的客户可以源码方式部署。
2. 仔细实战测试过，保证核心功能稳定可靠。

## 不承诺

免费版不承诺任何环境都有效，不提供任何技术服务，无论任何原因引发的任何问题，都不负任何责任。**请务必在测试环境完美演练后，再谨慎部署到生产环境。**

# 部署方式

## 模式一：直接安装在WEB服务器上

服务器原HTTP端口80改为其他如81，原HTTPS端口443改为4433，然后WAF占用80、443即可。

**WAF（80)<------------->127.0.0.1:81**

**WAF（443)<-------->127.0.0.1:4433**

测试正常后，81和4433端口不向公网开放。

## 模式二：独立部署，反向代理后端WEB服务器

像阿里云WAF可以在任何公网IP上安装，如WAF在北京，保护上海源站点：

**北京123.112.0.8（80)<-----> 202.96.20.1(上海80端口)**

**北京123.112.0.8（443端口)<-----> 202.96.20.1(上海443端口)**

也可以像硬件WAF在内网机房部署，保护源站WEB服务：

**内网WAF 192.168.1.8（80端口)<----->WEB服务器192.168.1.5(80端口)**

**内网WAF 192.168.1.8（443端口)<-----> WEB服务器192.168.1.5(443端口)**

实战环境最后还要修改DNS或者路由器NAT，指向WAF的IP。

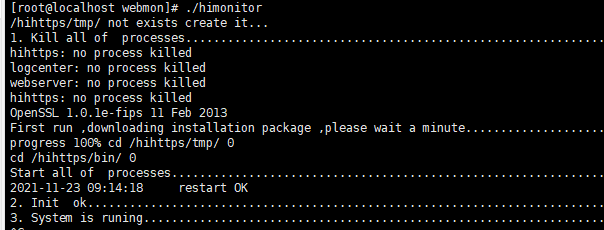
## 安装步骤

**himonitor集安装、启动、状态监控、停止于一体，**保证系统可以上互联网，并且80、443和9999端口没有被占用，以root权限，运行下面命令：

chmod +x ./himonitor

./himonitor

首次运行要下载最新版本，大约需要1分钟时间，如果出现下图三个步骤，打印出了 3.System is running.....，代表已经安装成功。



## 运行、停止和卸载

启动运行: ./himonitor

后台模式运行: ./himonitor daemon

停止运行: ./himonitor stop

卸载 : rm /hihttps/ -rf

默认没加开机启动，请自行把himonitor加入服务器开机启动程序。

# WEB管理

## 登录

管理口是9999端口，在浏览器上输入WAF的IP如http://192.168.1.8:9999/即可看到登录页面，用户名是admin 密码默认是admin ，登录进入主页后，请在顶上右边菜单尽快修改密码。

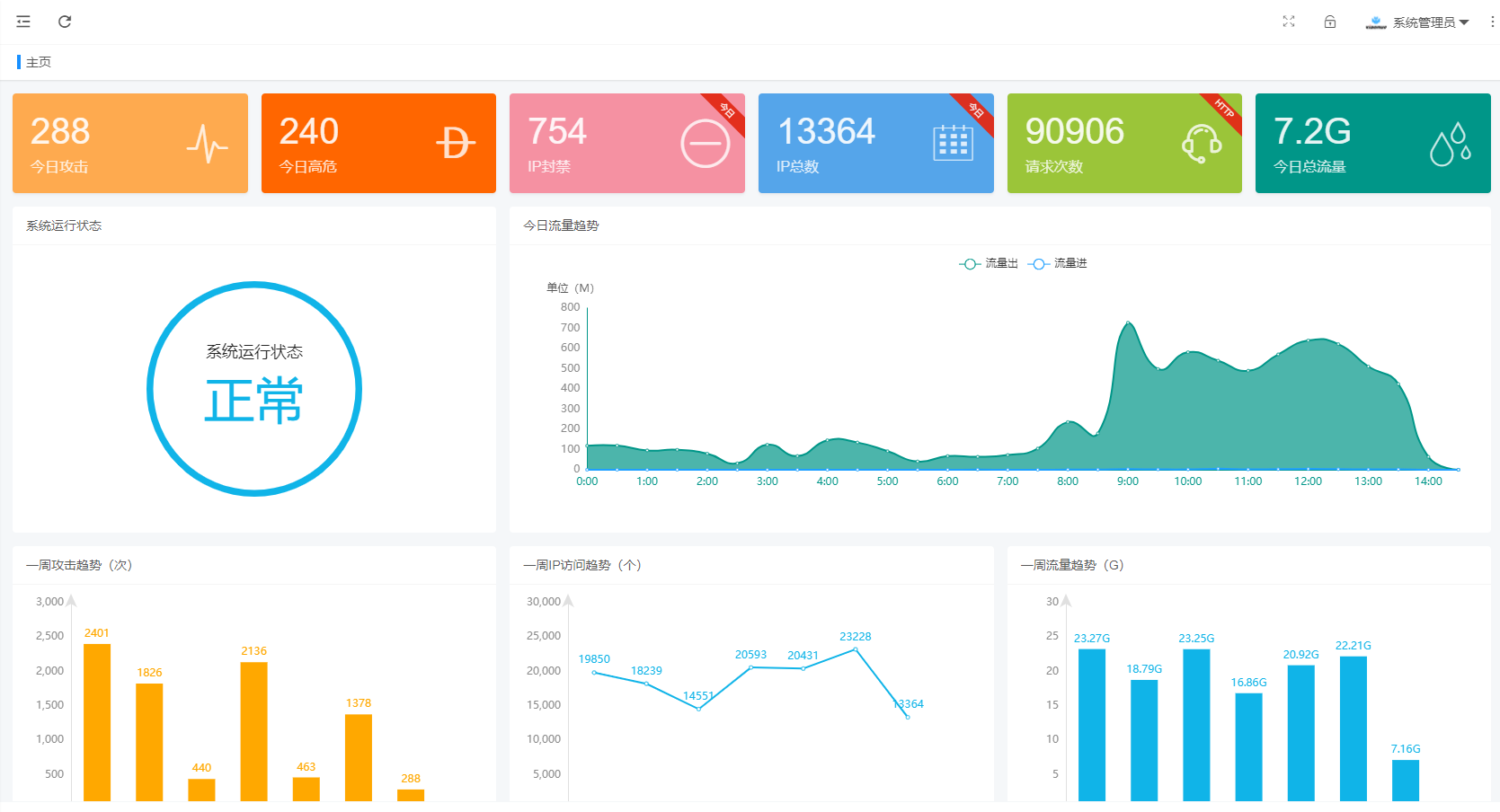


## 主页

登录后进入主页，其中系统运行状态，务必是正常。如果系统状态显示异常，通常原因是：

1、 80、443端口被其他程序如nginx占用，解决方法是改端口。

2、 SSL证书设置不对，或者OpenSSL未安装。



点击主页顶上的数据统计栏，可以直接进入相关日志（如攻击日志、IP流量统计等），其中：攻击日志是实时产生的，主页的其他数据统计、流量趋势、请求统计等大约有30秒左右的延迟。

# 基本设置

## 服务器设置



1. 如果WAF安装在WEB服务器上，只需要把默认的127.0.0.1对应的端口改为真实WEB服务端口如81，整个配置就完成了。(如果UI没自动刷新，请再次点击左边菜单）
2. 如果WAF是独立安装，一般来说，HTTP 80端口对应真实WEB服务器的80端口，HTTPS 443对应服务器的443端口。（具体原理参考第2节的部署方式）
3. WAF默认提供一张有证书给HTTPS服务，如果要更换证书，请把公钥和私钥放在同一个server.pem的文件中，再上传替换，证书错误同样会导致系统异常。正确的证书文件内容如下所示（有公钥和私钥）：

-----BEGIN CERTIFICATE-----

MIIEYDCCA0igAwIBAgIJALUqHsFBHJi/MA0GCSqGSIb3DQEBCwUAMIGiMQswCQzE1MFoXDTQwMDUyNDA1MzE1MFowgaQxMB0GA1UdDgQWBBT+4eKKFbOQvDaxWahSBkUdYuDKyDAOBgNVHQ8BAf8EBAMCAYIwOzw1/6lHSSmYbJ.........

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

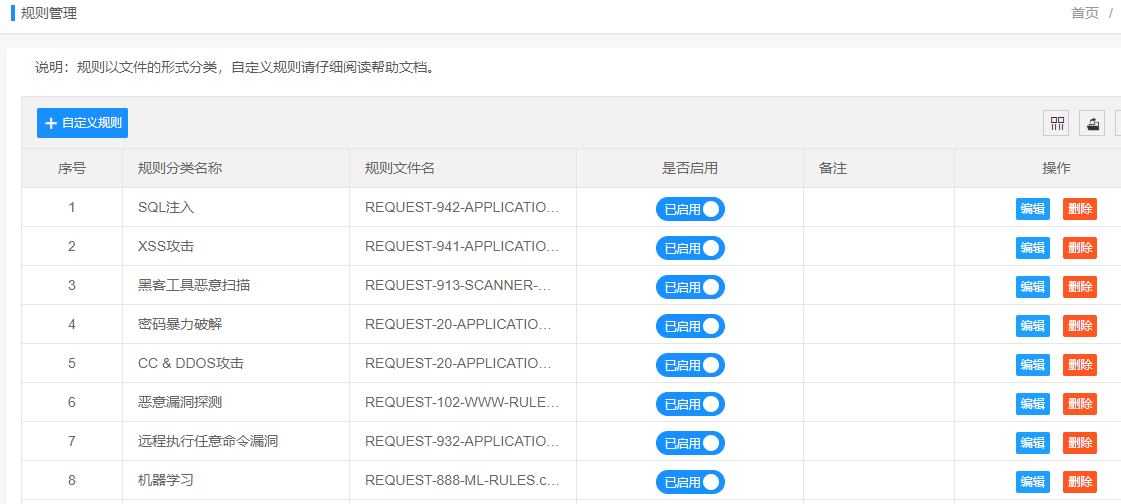
MIIEowIBAAKCAQEAsJQ6HRVofPGVsiEYLsW4jBJbppg1etY0/23KcI/xZGl3EsRx

q5DFCmsCmhYKE0LpP6nK/AWlrMuPUCVaooTtfhMiKAUOh19sytjsKnLD9aCftQDe1YaIdbVttrclARdaldJqi+t81ZjnlNjZfUjW3DBNyjsfGqZ6JR6.........

-----END RSA PRIVATE KEY-----

如果证书上载提示接口失败，可能身份过期，清除浏览器缓存，重新登录再试。

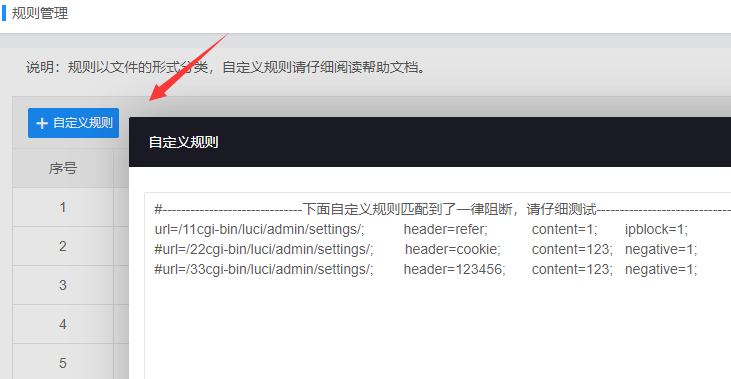
## 规则管理



系统默认提供了9类有明显特征的攻击规则，一般情况下，这几类规则非专业人员，一般不用做任何改动。

## 自定义规则

有些行为如爬虫、盗链、低频CC等没明显特征的，需要自定义规则来进行防御，建议由专业人员来进行编写。



**自定义规则每行一条，都是小写；无论系统规则是否设置为报警或者阻断模式，都一律是阻断。一定仔细测试后，再部署生产环境。**关键字定义如下如下：

url是http请求的地址，最大100字节；

header是http协议头，如get、cookie、referer、user-agent等头部，默认不写代表检查get头后面的url和参数，最大60字节。

content是匹配关键字，支持正则表达式，最大60字节。

ipblock默认0，1代表同时封禁IP。

negative默认0，1代表匹配结果取反，没有匹配到就阻断的意思。

每个关键字之间用分号;隔开，首字母#表示注释，下面先从HTTP协议头举例说明，假如从溯源日志里面，发现一个HTTP请求是这样：

GET /api/login.jsp?User=admin&password=123 HTTP/1.1

cache-control: no-cache

pragma: no-cache

accept: \*/\*

accept-encoding: gzip, deflate

from: bingbot(at)microsoft.com

host: [www.server.com](http://www.abc.com)

referer: http://www.baidu.com/cache?Id=3344433

user-agent: Mozilla/5.0 (compatible; spider/2.0; +http://www.baidu.com/search.htm)

connection: close

假如我们认为上面的请求是一个攻击，那么下面的规则分别代表：

url=/api/login.jsp;content=admin;ipblock=0;negative=0;

表示凡是url后面的参数中带有关键字admin的一律阻断。

url=/api/login.jsp;content=admin;ipblock=1;negative=0;

表示凡是url后面的参数中带有关键字admin的一律阻断并封禁IP。

url=/api/login.jsp;content=admin;ipblock=0;negative=1;

表示凡是url后面的参数中没有关键字admin的一律阻断。

url=/api/login.jsp;header=user-agent;content=spider;ipblock=1;

表示如果user-agent含有关键字spider的一律阻断，用于阻断并封禁有特征的爬虫。

url=/api/login.jsp;header=cookie;content=admin;negative=1;

表示如果没有cookie或者cookie中没有关键字admin的一律阻断。（可以给爬虫设置cookie陷阱，精准封禁IP）

url=/api/login.jsp;header=referer;content=server.com;ipblock=1;negative=1;

表示如果没有referer或者referer不含关键字server.com的一律封禁IP，用于防盗链。

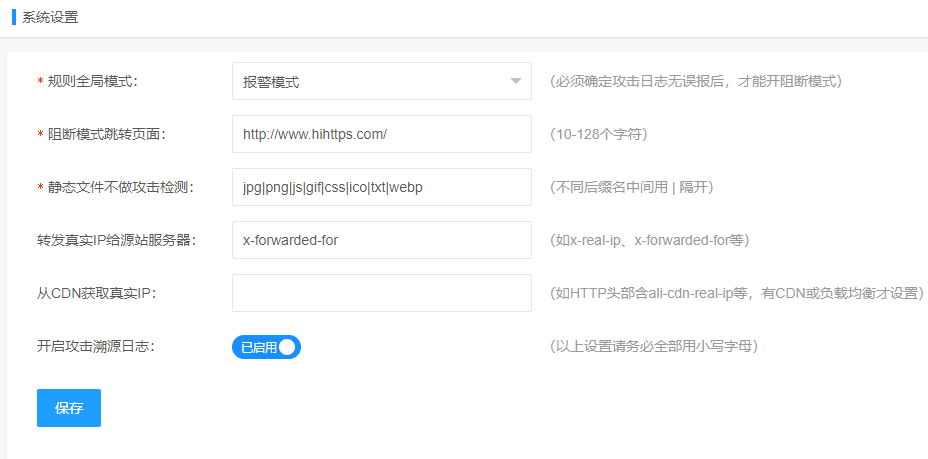
url=/;content=123456;ipblock=0;negative=0;

表示任意url及其后面的参数中带有关键字123456的一律阻断。

WAF其实支持更复杂的规则如检查body参数、文件上传等，并且兼容ModSecurity规范，由于复杂我们以人工技术服务的方式定制，这里就不一一赘述了，有兴趣的用户可以自行研究/hihttps/rules/目录下的规则或者访问知乎参考这篇文章自定义规则防御思想https://zhuanlan.zhihu.com/p/351261252。

自定义规则保存后，要点击重启才能生效。

## 系统设置



WAF默认是报警模式，理论上不影响真实WEB服务器的业务，**必须在攻击日志里面仔细确认无误报，才能开启阻断模式。**一般来说，WAF前三天不误报，之后也几乎不会误报。

如果WAF的前面有CDN或者负载均衡，那么WAF拿到的IP地址都是CDN的IP，无法直接获取到真实的用户IP地址（不能准确阻断恶意IP），那么只能在HTTP头部的自定义字段获取用户IP。

系统设置里面所有的配置都是小写字母。

## IP封禁设置



即使规则设置了阻断，也不会封禁恶意IP，系统会用人工智能的方式发现恶意IP，包括：

1. 多次触发危险攻击规则。
2. 使用漏洞扫描器。
3. 低频或者高频CC恶意攻击.......等情况。

**默认是报警模式，必须仔细确定攻击日志和封禁日志，没有误报才能开启阻断模式，默认阻断恶意IP半个小时。**

# 黑白名单

白名单的主要作用是解决个别特殊的情况下产生的误报，比如有程序员不按规范，写的WEB接口特征和SQL注入规则特征几乎一样，那么就可能产生误报甚至误封IP，那么就用白名单的方式解决，黑名单一般不用。

## URL白名单



这里可以添加或者编辑不做攻击检测的URL接口地址，用全小写字母，比如上面设置，凡是以/hihttps/whitelist开头的URL，都会匹配成功，最大支持16条白名单。

## IP白名单



有些很特殊的IP，如内网或者NAT转换的攻击概率小，可以设置为白名单模式不做攻击检测，最大16条规则。格式是IP和掩码，如:

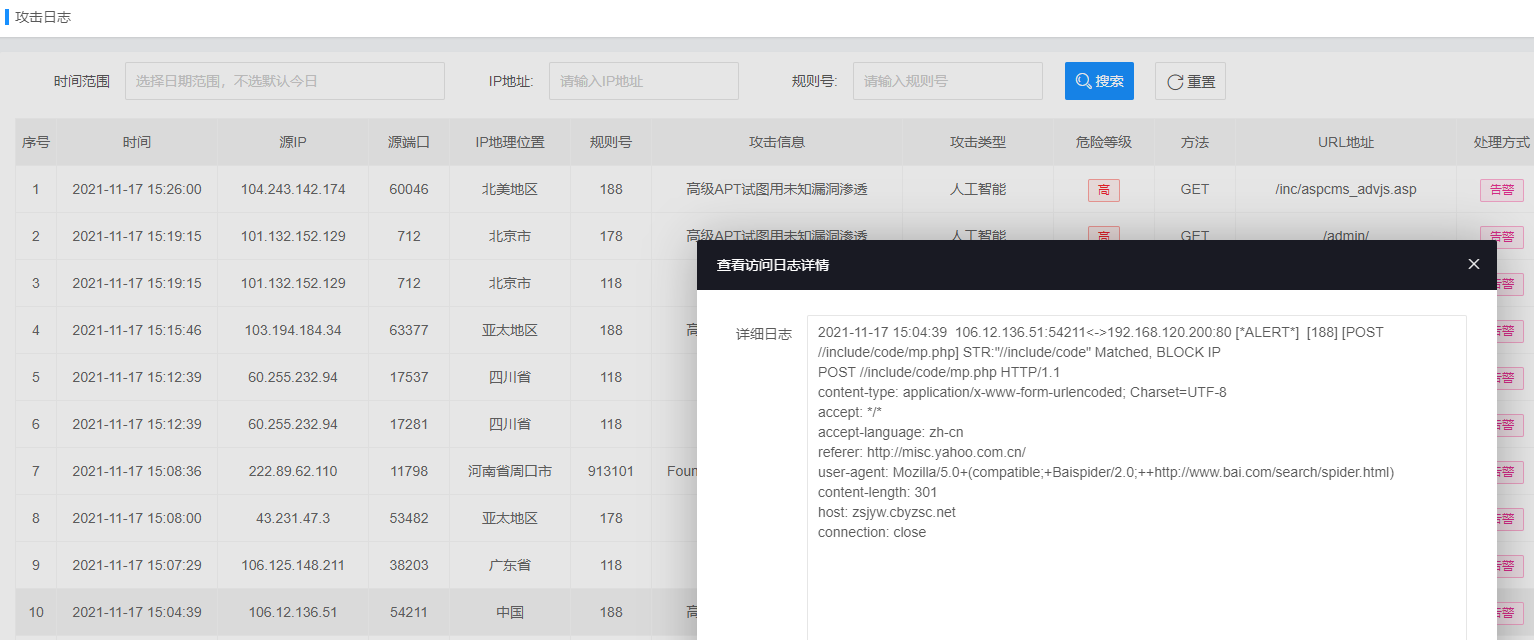
192.168.1.88/32 表示只有192.168.1.88这个IP是白名单。

192.168.1.0/24表示只有192.168.1.0-192.168.1.255这个IP范围都是白名单。

192.168.0.0/16表示只有192.168.0.0-192.168.255.255这个IP范围都是白名单。

# 日志查看

## 攻击日志



**攻击日志是实时的，点击“攻击日志”菜单或者“搜索”按钮，都可以刷新最新的日志**，也可以按日期、IP地址和规则号进行搜索，WAF刚部署的前三天，建议仔细观察每条日志，确定没误报后，开启阻断和IP封禁。

如果是测试功能，可以向WAF的IP地址（下面192.168.1.8换成您的真实WAF的IP)发送攻击测试：

1、SQL注入：http://192.168.1.8/index.html?id=123' or 1='1

2、XSS：http://192.168.1.8/index.html?id=<script>alert(1);</script>

3、任意漏洞扫描器如Kali Linux里面的工具nikto：

nikto -h 192.168.1.8 -port 80 -C all

nikto -h 192.168.1.8 -ssl -port 443 -C all

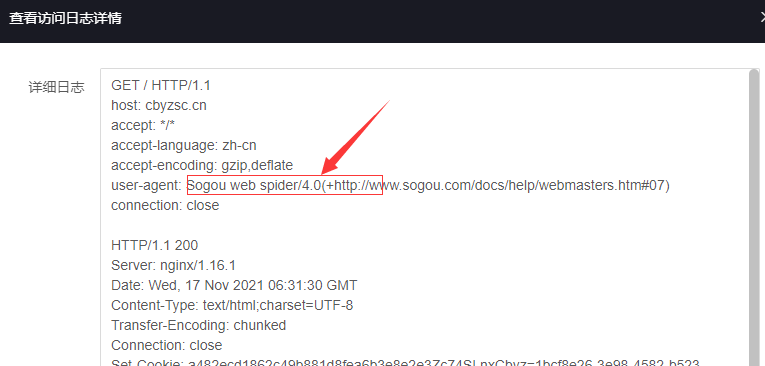
4、DDOS和CC可以用http压力测试工具wrk：

wrk -c 10 -t 10 -d 10 http://192.168.1.8/

注意：如果IP封禁是阻断模式，用nikto 和wrk高并发扫描，WAF会阻断IP，攻击日志数量会远远小于报警模式，主页的统计数字有30秒左右延迟是正常的。

## 溯源日志

溯源日志是记录除静态文件（如图片、CSS等）以外的全部HTTP请求日志，用以人工分析某些IP是否有恶意行为，如果有，在溯源日志详情里面发现特征，编写自定义规则进行对抗防御。



如上图可能是恶意爬虫，如果量大影响了正常的网站，我们就可以通过自定义检测user-agent的规则进行阻断。

## 封禁日志

封禁日志是根据IP黑名单和攻击日志而产生的危险攻击IP，默认只是报警，不会封禁。WAF上线三天内，务必仔细检查，没有误报才能设置IP封禁为阻断模式。个别误报，一般用白名单URL方式解决。

## 未知漏洞【收费】

绝大多数攻击对系统是无害的，但未知攻击特别是0day漏洞，对系统的危害巨大，HTTPWAF的目标就是用算法及时发现未知漏洞。技术过于超前，收费才提供。

# 统计分析

## IP流量统计



WAF按流量多少统计出排行前1000名的IP地址，这个非常重要，WAF会标记出对于流量异常和有攻击的IP，这些异常流量最好人工查看溯源日志，究竟发生了什么。

**我们提倡在先在流量里面，整体看是否有攻击误报或者流量异常，然后在进一步配合业务自定义防御规则**。

## URL分析统计

和流量一样，系统统计出排行前1000名的URL访问，系统管理员根据业务自身情况，判断是否有恶意攻击，然后自定义规则进行防御。

## 十大攻击源

查询出指定时间内的十大攻击源IP。

# 系统管理

## 远程管理



WAF的9999端口默认允许任意IP访问(0.0.0.0/0)，为了保证安全，禁止向公网用户开放。最好在边界防火墙上配置9999端口的访问范围，如果在这里设置不正确，WAF可能无法访问，会返回“aha, aihttps is here” 的禁止访问提示。

如果万一设置错误，解决方法是重装WAF。

## 恢复出厂设置

如果做了错误的配置，可以用点击这个按钮，恢复到原始安装状态。

## 系统重启

某些情况下，如增加了自定义规则、替换了数字证书等，要重启才能生效。重启过程一般在几秒完成，重启后，务必刷新主页查看运行状态，显示正常代表配置正确。

# 开机启动

开机自启动请自行编写脚本启动/hihttps/update/himonitor程序，WAF安装后，不会改动系统配置。

/hihttps/update/himonitor daemon是以后台守护进程的方式启动。

# 开放源码

HTTPWAF收费版是专注用各类算法对抗未知攻击，尤其以发现0day漏洞为目标，源码可以开放，微信号httpwaf。



攻防乃顶级智商对抗，我们努力做最好用的WAF，9999管理端口禁止向公网开放，勿谓言之不预也。